a.) Amendments to Specification

Replace the paragraph beginning at page 1, line 12, in the specification as originally filed, with the following rewritten paragraph:

--With advances in integrated circuit, microprocessor, networking and communication technologies, increasing ~~number~~ numbers of devices, in particular, digital computing devices, are being networked together. Devices are often first coupled to a local area network, such as an Ethernet based office/home network. In turn, local area networks are interconnected together through wide area networks, such as ATM networks, Frame Relays, and the like. Of particular ~~notoriety~~ interest is the TCP/IP based global inter-networks, Internet.--

Replace the paragraph beginning at page 1, line 19 and continuing through page 2, line2, in the specification as originally filed, with the following rewritten paragraph:

--As a result of this trend of increased connectivity, increasing numbers of applications that are network dependent are being deployed. Examples of these network dependent applications include but are not limited to, email, net-based telephony, world wide web and various types of e-commerce. For these applications, success inherently means a high volume of desirable network traffic for their implementing servers. To ensure continuing success, quality of service through orderly and efficient handling of the large volume of desirable network traffic has become of paramount importance. Various subject matters, such as scalability, distributive deployment and caching of contents as well as regulating network traffic destined for a network node, have become of great interest to the artesian.--

Replace the paragraph beginning at page 2, line 10, in the specification as originally filed, with the following rewritten paragraph:

--However, to-date, there is no known effective approach to detecting and filtering out packets with spoof source addresses. What is particularly difficult about detecting and filtering out packets with spoof source addresses is the fact that often times spoof instances are intermixed with non-spoof instances. For example, source address

128.128.128.16 may be an authentic source address, but it is also one of the spoof addresses employed by a denial of service attacker. As a result, while" most likely an overwhelming majority of the packets with this source address are spoof instances, there could still be a significant number of packets with this source address that are non-spoof instances.--

Replace the paragraph beginning at page 4, line 15 and continuing through page 5, line 2, in the specification as originally filed, with the following rewritten paragraph:

--The director makes its determinations based at least in part on a selected one of a number of consistency measures. The consistency measures may include but are not limited to, spatial consistency, destination consistency, migration consistency, and ~~temporary~~ temporal consistency. The consistency measures are evaluated using spatial, destination source address range, migration, and timing (S/D/M/T) distribution profiles of the reported source addresses. In some embodiments, the determinations are based further in view of reference S/D/M/T distribution profiles. In one embodiment, the reference S/D/M/T distribution profile is an exemplary S/D/M/T distribution profile of a typical non-spoof source address, while in another embodiment, it is a historical S/D/M/T distribution profile of the source address. In various embodiments, all or portions of the packets with source addresses having S/D/M/T distribution profiles that do not substantially resemble the reference S/D/M/T distribution profiles are deemed to be packets with spoof source addresses.--

Replace the paragraph beginning at page 7, line 23 and continuing through page 8, line 6, in the specification as originally filed, with the following rewritten paragraph:

--Referring now first to Figures 1-2, wherein two block diagrams illustrating a network view and a method view of the present invention, in accordance with one embodiment, are shown. As illustrated in Fig 1, in accordance with the present invention, network 100 is provided with director 102 to assist in fending off undesirable network traffic destined for a network node of network 100, such as server 110, to assist in ensuring quality of service provided by the network node. More specifically, director 102 detects packets with spoof source addresses, and determines whether filtering actions

are to be deployed to filter out such packets from network 100. Director 102 advantageously performs the detection and determination, based at least in part on one or more consistency measures.--

Replace the paragraph beginning at page 8, line 24 and continuing through page 9, line 5, in the specification as originally filed, with the following rewritten paragraph:

--In various embodiments, director 102 evaluates these consistency metrics using spatial, destination source address range, migration and timing (SDMT) distribution profiles. Director 102 constructs and compares the SDMT distribution profiles to reference SDMT distribution profiles of the source addresses. In one embodiment, the reference SDMT distribution profiles are exemplary SDMT distribution profiles for non-spoof source addresses in general. In another embodiment, the reference SDMT distribution profiles are historical SDMT distribution profiles for specific source addresses.

Replace the paragraph beginning at page 12, line 22 and continuing through page 13, line 18, in the specification as originally filed, with the following rewritten paragraph:

--Skipping briefly to Fig. 13a-13d and Fig. 14a-14d, Fig. 13a-13b illustrate one each of an example spatial and an example "destination" distribution profile of a source address having spoof instances. Experience has shown that if spoof source addresses are employed in a denial of service attacks against a network node, it is likely that the source addresses will be simultaneously observed in multiple domains of network 100, even domains that are geographically dispersed, as illustrated by the histogram of Fig. 13a. Similarly, if spoof source addresses are employed in a denial of service attacks against a network node, it is likely that the spoof source addresses will not be a subset or substantially related to the source addresses of other packets being routed to other destinations at the routing location, as illustrated by Fig. 13b, where the destinations have disjointed source address ranges for the various destinations of the packets being routed at the routing location. Further, if spoof source addresses are employed in a denial of service attacks against a network node, it is likely that the spoof source addresses will be migrating across different network domains in a very rapid rate, i.e. the routing paths

change from one network domain to another relatively quickly, as illustrated by Fig. 13c, having a high number of incidence with short timing duration between routing path changes. Lastly, if spoof source addresses are employed in a denial of service attacks against a network node, it is likely that the source addresses will be repeatedly observed within a very short interval as illustrated by the histogram of Fig. ~~13b~~ 13d, having an exponentially decay type of profile (in terms of elapsed time between packets with the same source address).--

Replace the paragraph beginning at page 14, line 10, in the specification as originally filed, with the following rewritten paragraph:

--Thus, a decision maker, such as director 102, may infer whether an observed source address is to be deemed as having spoof source address instances based on whether the observed S/D/M/T distribution profile of the source address substantial resembles that of a reference S/D/M/T distribution profile or not. Substantial resemblance may be quantitatively determined using any one of a number of known statistical techniques, e.g. the least square fitness test. The threshold for inferring a source address as having spoof source address instances is application dependent, depending on whether for a particular network node, it is more suitable to err on the side of incorrectly inferring a non-spoof source address as having spoof source address instance, or it is more suitable to err on the side of failing to detect some of the spoof source address instances. The former preference will tend to lead to over filtering, rejecting more packets than necessary, while the later preference will tend to lead to under filtering, resulting in more undesirable packets to "hit" the network node.--

Replace the paragraph beginning at page 17, line 23 and continuing through page 18, line 2, in the specification as originally filed, with the following rewritten paragraph:

--For report function 304, as illustrated in ~~fig.~~ Fig. 5, in like manner, upon start up, it awaits ~~for~~ the expiration of a timer, block 502. Likewise, the periodicity of expiration is application dependent. Upon expiration, i.e. time for reporting, report function 304 reports all or a predetermined subset (e.g. the most frequently observed

subsets) of cached source addresses to director 102, as earlier described, blocks 504-506. Upon transmission, report function 304 returns to block 502.--

Replace the paragraph beginning at page 20, line 18 and continuing through page 21, line 15, in the specification as originally filed, with the following rewritten paragraph:

--As illustrated in ~~fig.~~ Fig. 10, upon start up, analyzer 804 selects a source address for analysis. At block 1002, analyzer 804 constructs a spatial, a destination source address range, a migration, and/or timing distribution profile for the source address being analyzed, using the reported data. Recall that a spatial distribution profile addresses the network domain distribution profiles of the reported source addresses. Destination source address range profiles address the source address ranges of other packets being routed to other destination at the reporting location. Migration profiles address the rapidity the routing paths change for the reported source addresses, and the timing distribution profiles addresses the rapidity with which packets with the reported source addresses are issued. At block 1004, analyzer 804 compares the constructed S/D/M/T distribution profiles to reference S/D/M/T distribution profiles. As described earlier, the reference S/D/M/T distribution profiles may be an exemplary reference S/D/M/T distribution profile for a non-spoof source address in general, or it may be a historical S/D/M/T distribution profile of the source address under analysis in particular. At ~~beek~~ block 1006, analyzer 804 determines if the source address under analysis should be deemed as having spoof instances, i.e. at least some of the packets observed are to be deemed as having spoof source addresses. As described earlier, the determination may be made using any one of a number statistical techniques in deciding whether the constructed S/D/M/T distribution profile bears sufficient resemblance to the reference S/D/M/T distribution profile. If the source address is not to be deemed as having spoof instances, no actions are taken. The process returns to block 1002 for another source address to be analyzed. However, if the source address is to be deemed as having spoof instances, analyzer 804 notifies/alerts regulator 806 accordingly, block 1008.--

This listing of claims will replace all prior versions and listings of claims in this application:

b.) Listing of Claims

1. (Original) A network comprising:

a plurality of network nodes;

a plurality of routing devices to route network traffics between selected ones of said network nodes; and

director coupled to said routing devices to determine whether selected instances of source addresses of packets routed by said routing devices are spoof source addresses, based at least in part on one or more consistency measures.

2. (Original) The network of claim 1, wherein the director bases said determination on at least spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile.

3. (Original) The network of claim 2, wherein said at least one reference source address spatial distribution profile comprises at least a selected one of an exemplary spatial distribution profile for a non-spoof source address in general, and a historical spatial distribution profile for a particular source address.

4. (Original) The network of claim 1, wherein the director bases said determination on at least destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference DSAR distribution profile.

5. (Original) The network of claim 4, wherein said at least one reference DSAR distribution profile comprises at least a selected one of an exemplary DSAR distribution profile for a non-spoof source address in general, and a historical DSAR distribution profile for a particular source address.

6. (Original) The network of claim 1, wherein the director bases said determination on at least migration distribution profiles of said source addresses, and in view of at least one reference migration distribution profile.

7. (Original) The network of claim 6, wherein said at least one reference migration distribution profile comprises at least a selected one of an exemplary migration distribution profile for a non-spoof source address in general, and a historical migration distribution profile for a particular source address.

8. (Original) The network of claim 1, wherein the director bases said determination on at least timing distribution profiles of said source addresses, and in view of at least one reference source address timing distribution profile.

9. (Original) The network of claim 8, wherein said at least one reference source address timing distribution profile comprises at least a selected one of an exemplary timing distribution profile for a non-spoof source address in general, and a historical timing distribution profile for a particular source address.

10. (Original) The network of claim 1, wherein the director is further equipped to determine whether filtering actions are to be taken to filter out packets with source addresses having instances deemed to be spoof source addresses, and if filtering actions are to taken, where among said routing devices, said filtering actions are to be taken.

11. (Original) The network of claim 10, wherein the director takes into consideration in making said where determination, where packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in said network.

12. (Original) The network of claim 1, wherein the director comprises a plurality of director devices cooperatively coupled to each other to jointly make said determination.

13. (Original) The network of claim 1, wherein the network further comprises a plurality of sensors, either integrally disposed in a subset of said routing devices or externally disposed and coupled to the subset of routing devices, to monitor and report on source addresses of packets routed through the subset of routing devices.

14. (Original) The network of claim 13, wherein the sensors are further equipped to facilitate application of desired source address based filtering on packets being routed through selected ones of said subset of routing devices.

15. (Original) A networking method comprising:

receiving information associated with source addresses of packets being routed to and from a plurality of network nodes of a network;

determining whether selected instances of said source addresses are spoof instances of said source addresses, based at least in part on one or more consistency measures; and

managing said network based at least in part on the results of said determination.

16. (Original) The method of claim 15, wherein said determination is made based at least in part on spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile.

17. (Currently amended) The method of claim 16, wherein said ~~determining~~ determination comprises constructing said spatial distribution profiles of said source addresses.

18. (Original) The method of claim 16, wherein said determining comprises determining whether each of the spatial distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profile.

19. (Original) The method of claim 16, wherein said at least one reference spatial distribution profile comprises at least a selected one of an exemplary spatial distribution profile for a non-spoof source address in general, and a historical spatial distribution profile for a particular source address.

20. (Original) The method of claim 15, wherein said determination is made based at least in part on destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference DSAR distribution profile.

21. (currently amended) The method of claim 20, wherein said ~~determining~~ determination comprises constructing said DSAR distribution profiles of said source addresses.

22. (Original) The method of claim 20, wherein said determining comprises determining whether each of the DSAR distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profile.

23. (Original) The method of claim 20, wherein said at least one reference DSAR distribution profile comprises at least a selected one of an exemplary DSAR distribution profile for a non-spoof source address in general, and a historical DSAR distribution profile for a particular source address.

24. (Original) The method of claim 15, wherein said determination is made based at least in part on migration distribution profiles of said source addresses, and in view of at least one reference migration distribution profile.

25. (Original) The method of claim 24, wherein said determining comprises constructing said migration distribution profiles of said source addresses.

26. (Original) The method of claim 24, wherein said determining comprises determining whether each of the migration distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profile.

27. (Original) The method of claim 24, wherein said at least one reference migration distribution profile comprises at least a selected one of an exemplary migration distribution profile for a non-spoof source address in general, and a historical migration distribution profile for a particular source address.

28. (Original) The method of claim 15, wherein said determination is made based on at least timing distribution profiles of said source addresses, and in view of at least one reference source address timing distribution profile.

29. (Original) The method of claim 28, wherein said determining comprises constructing said timing distribution profiles of said source addresses.

30. (Original) The method of claim 28, wherein said determining comprises determining whether each of the timing distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profile.

31. (Original) The method of claim 28, wherein said at least one reference timing distribution profile comprises at least a selected one of an exemplary timing distribution profile for a non-spoof source address in general, and a historical timing distribution profile for a particular source address.

32. (Original) The method of claim 15, wherein said managing comprises determining whether filtering actions are to be taken in said network to filter out at least some packets

having source addresses deemed to be having spoof instances, and if filtering actions are to be taken, where among a plurality of routing devices, said filtering actions are to be taken.

33. (Original) The method of claim 32, wherein said where determination comprises taking into consideration where packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in said network.

34. (Currently amended) An apparatus comprising:

(a) a storage medium having stored therein a plurality of programming instructions designed to implement a director to receive reporting of information associated with source addresses of packets routed through a plurality of routing devices of a network, and to determine whether at least some instances of said source addresses are spoof instances <u>based on at least spatial distribution profiles of said source addresses, and in view of at least one reference source address spatial distribution profile</u>; and

(b) a processor coupled the storage medium to execute the programming instructions.

35. (Cancelled)

36. (currently amended) The apparatus of claim ~~35~~ <u>34</u>, wherein said programming instructions are designed to be able to construct said spatial distribution profiles of said source addresses.

37. (currently amended) The apparatus of claim ~~35~~ <u>34</u>, wherein said programming instructions are designed to be able to determine whether each of the spatial distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profile.

38. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least destination source address range (DSAR) distribution profiles of said source addresses, and in view of at least one reference source address DSAR distribution profile.

39. (Original) The apparatus of claim 38, wherein said programming instructions are designed to be able to construct said DSAR distribution profiles of said source addresses.

40. (Original) The apparatus of claim 38, wherein said programming instructions are designed to be able to determine whether each of the DSAR distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profile.

41. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least migration distribution profiles of said source addresses, and in view of at least one reference source address migration distribution profile.

42. (Original) The apparatus of claim 41, wherein said programming instructions are designed to be able to construct said migration distribution profiles of said source addresses.

43. (Original) The apparatus of claim 41, wherein said programming instructions are designed to be able to determine whether each of the migration distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profile.

44. (Original) The apparatus of claim 34, wherein said programming instructions are designed to make said determination based on at least timing distribution profiles of said

source addresses, and in view of at least one reference source address timing distribution profile.

45. (Original) The apparatus of claim 44, wherein said programming instructions are designed to be able to construct said timing distribution profiles of said source addresses.

46. (Original) The apparatus of claim 44, wherein said programming instructions are designed to be able to determine whether each of the timing distribution profiles of the source addresses is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profile.

47. (Original) The apparatus of claim 34, wherein said programming instructions are designed to be able to determine whether filtering actions are to be taken in said network to filter out at least some packets having source addresses deemed to be having spoof instances, and if filtering actions are to be taken, further determine where among a plurality of routing devices, said filtering actions are to be taken.

48. (Original) The apparatus of claim 47, wherein said programming instructions are designed to take into consideration where packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in said network, when making said where determination.